

40



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/505,951	02/15/2000	Simon Robert Walmsley	AUTH08US	5608

7590 02/17/2005  
 Kia Silverbrook  
 Silverbrook Research Pty Ltd  
 393 Darling Street  
 Balmain, 2041  
 AUSTRALIA

EXAMINER

DAVIS, ZACHARY A

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 02/17/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center"><b>Office Action Summary</b></p>	<b>Application No.</b> 09/505,951	<b>Applicant(s)</b> WALMSLEY ET AL.	
	<b>Examiner</b> Zachary A Davis	<b>Art Unit</b> 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 13 October 2004.  
 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.  
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-20 is/are pending in the application.  
     4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
 6) ☒ Claim(s) 1-20 is/are rejected.  
 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.  
 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
     a) ☐ All    b) ☐ Some \*    c) ☐ None of:  
         1. ☐ Certified copies of the priority documents have been received.  
         2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
         3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
     \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. An amendment was received on 13 October 2004. No claims have been amended, added, or canceled. Claims 1-20 are currently pending in the present application.

### *Response to Arguments*

2. Applicant's arguments filed 13 October have been fully considered but they are not persuasive.

In response to Applicant's arguments against the references individually, specifically the arguments against Hoffmann et al, US Patent 5608800, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

In response to Applicant's argument that there is no suggestion to combine the references, the Examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation to

combine was stated in the previous Office action; namely, to allow the detection of the unauthorized introduction of data into the transmitted data (see Hoffmann, column 1, line 61-column 2, line 6). In other words, the combination would assist in the detection of an unauthorized or unauthenticated party.

Regarding the reference by Sony Corporation, EP 0817420, Applicant asserts that Sony describes a mutual authentication method with two untrusted IC cards, citing the abstract. The Examiner agrees that Sony does state that mutual authentication is performed; however, the Examiner does not agree with the assertion that there are two untrusted IC cards. Sony discloses that the protocol is performed between one IC card and a reader/writer, which correspond to the untrusted and trusted authentication chips, respectively, of claim 1 of the present application (see Abstract).

Further in reference to Sony, Applicant argues that Sony does not disclose encrypting and decrypting data in the trusted and untrusted authentication chips. However, the Examiner believes that Sony does indeed disclose that encryption and decryption are performed in each of the trusted chip, i.e. the reader/writer; and the untrusted chip, i.e. the IC card (see Figure 9).

Applicant further argues that Hoffmann does not teach or suggest calculating a signature for a random number using a signature function, and that Hoffmann instead teaches encrypting the random data with a transfer key. While the Examiner agrees that Hoffmann discloses that the random data may be enciphered with a transfer key (column 2, lines 25-27, as cited by Applicant), the Examiner also believes that Hoffmann

does disclose that the random data is indeed part of the signature that is formed (see column 3, lines 40-45; see also Figure 3).

Therefore, for the above reasons, the rejections of the claims, as detailed below, are maintained.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-4, 6-15, and 17-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sony Corporation (Kusakabe), European Patent EP 0817420, in view of Hoffmann et al, US Patent 5608800.

In reference to Claim 1, Sony discloses an authentication method (see Figures 7-9, Claim 1, and column 2, line 49-column 3, line 17) in which a random number is generated (column 8, lines 12-17) and encrypted with a symmetric encryption function using a first key in a first apparatus (column 9, lines 13-17). The encrypted random number is sent to a second apparatus (column 9, lines 18-21) and decrypted with a symmetric decryption function using the first key (column 9, lines 31-37), and then encrypted with the symmetric encryption function using a second key (column 9, lines 41-48) and sent to the first apparatus (column 9, line 57-column 10, line 2). The

encrypted random number is compared with the originally encrypted random number (column 10, lines 29-31) after first being decrypted with the symmetric decryption function using the second key (column 10, lines 21-28). The two numbers matching authenticates the second apparatus (column 10, lines 31-35) and the two numbers not matching does not authenticate the second apparatus (column 10, lines 36-39). However, Sony does not disclose the calculation and comparison of a digital signature as a step of the authentication method.

Hoffmann discloses an authentication method that includes generating a digital signature in a first apparatus (column 3, lines 25-27) and verifying that signature in a second apparatus (column 4, lines 6-7). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as disclosed by Sony by including the steps of generating a signature in the first apparatus and verifying the signature in the second apparatus, in order to be able to detect the unauthorized introduction of data into the transmitted encrypted data (column 1, line 61-column 2, line 6).

Further, it follows logically from the combination of Sony as modified by Hoffmann, that the signature of Hoffmann would be performed on the random number of Sony, and that the random number and the signature would be encrypted together under the same first symmetric key in the first device. Similarly, it follows logically that the signature would be decrypted in the second device using the first symmetric key at the same time the random number is decrypted.

In reference to Claim 2, Sony further discloses that the first and second keys are held in both the first and second apparatuses (see Figure 9).

In reference to Claim 3, Sony further discloses that the first apparatus contains a random function to generate random numbers (column 8, lines 12-15).

In reference to Claim 4, Sony further discloses that the second apparatus holds a decryption function (column 9, lines 31-37).

In reference to Claim 6, Sony further discloses that the second apparatus decrypts the random number with the first key (column 9, lines 31-37), encrypts the random number with the second key (column 9, lines 41-48), and sends the encrypted random number to the first apparatus (column 9, line 57-column 10, line 2).

Additionally, Hoffmann further discloses verifying the signature in the second apparatus (column 4, lines 6-7).

In reference to Claim 7, Sony further discloses that the second apparatus monitors the time elapsed between steps of its processing (column 10, lines 53-56).

In reference to Claim 8, Sony further discloses that the function generating the random numbers is held in the first apparatus (column 8, lines 12-15). Additionally, Sony discloses that if the second apparatus is not authenticated, the authentication process is terminated (column 10, lines 36-39).

In reference to Claim 9, Sony further discloses that the first apparatus monitors the time elapsed between steps of its processing (column 10, lines 6-7).

In reference to Claim 10, Sony further discloses that it is determined if the second apparatus is valid (column 10, lines 31-35) or not (column 10, lines 36-39).

Claims 11-15 and 17-20 are system claims corresponding substantially to the method steps of Claims 1-4 and 6-10, and are thus rejected by a similar rationale.

5. Claims 5 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sony in view of Hoffmann as applied to claims 1 and 11 above, respectively, and further in view of Schneier, *Applied Cryptography*.

Sony as modified by Hoffmann discloses everything as applied to Claims 1 and 11 above. However, Sony does not disclose the use of digital signatures, and Hoffmann does not explicitly disclose the use of digital signatures of 160 bits.

Schneier discloses that hash functions can be used in the creation of digital signatures, and specifically discloses the use of 160 bit hashes (page 38, last paragraph).

Therefore, it would have been obvious to modify the method of Sony as modified by Hoffmann to include digital signatures 160 bits in length in order to increase the speed of the signature algorithm (see Schneier, page 38, last paragraph-page 39, first full paragraph).

### ***Conclusion***

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).



A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

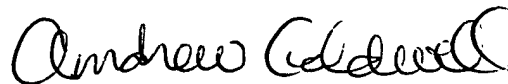
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ZAD  
zad



**ANDREW CALDWELL**  
**SUPERVISORY PATENT EXAMINER**